New wave of ransomware from Russian-led hackers: researchers

June 26 2020

Two Russian nationals indicted on charges of hacking in December are believed to be behind a new ransomware scheme targeting US firms, according to security experts

Russia-based hackers are stepping up ransomware attacks against major

US firms seeking to cripple computer networks if their demands for millions of dollars are not met, security researchers are warning.

The cybersecurity firm Symantec on Thursday said it had identified at least 31 targets in the United States, including eight Fortune 500 companies.

"The attackers behind this threat appear to be skilled and experienced, capable of penetrating some of the most well protected corporations, stealing credentials, and moving with ease across their networks. As such, WastedLocker is a highly dangerous piece of ransomware," said the threat intelligence team of Broadcom-owned Symantec in its alert.

"At least 31 customer organizations have been attacked, meaning the total number of attacks may be much higher. The attackers had breached the networks of targeted organizations and were in the process of laying the groundwork for staging ransomware attacks."

Earlier in the week, a similar warning came from the British-based security firm NCC Group, which identified the ransomware strain dubbed WastedLocker as a new threat since May.

The researchers said those behind the attacks include two Russian nationals, Igor Olegovich Turashev and Maksim Viktorovich Yakubets, indicted in the United States in December for their involvement in an entity known as Evil Corp which is accused of hacking US and British banks.

NCC analyst Stefano Antenucci wrote that researchers can show "with high confidence" that the latest ransomware is from Evil Corp, which has been using the so-called Dridex malware since July 2014.

The US indictment alleges the group believed to be linked to Russian

intelligence inserted malware on computers in dozens of countries to steal more than $100 million from companies and local authorities.

The indictment was accompanied by sanctions from the US Treasury on the two men, as well as the announcement of a $5 million reward toward Yakubets' arrest and conviction—the highest reward ever offered for a cybercriminal.

The Infraud Organization touted itself with the slogan 'In Fraud We Trust'

Hacker pleads guilty

The warnings came as another Russian hacker named as one of the leaders of a global cybercrime empire pleaded guilty to conspiracy in a

Nevada court Friday, according to the Department of Justice, two years after he was arrested in Thailand.

Sergey Medvedev, 33, has previously been described as a co-administrator of the Infraud Organization, an online network that stole and sold credit card and other personal identity data, causing $530 million in losses, according to US authorities.

The hacker, who worked under names including "serjbear" and "Stells", was arrested in Bangkok in February 2018 after masked cops armed with automatic weapons swooped on his condo. He was later extradited to the United States.

Infraud was founded in Ukraine in 2010 and touted itself with the slogan "In Fraud We Trust."

It became the "premier destination" on the web for purchasing goods with counterfeit or stolen credit card information, according to US authorities.

The organization, which had 10,901 approved "members" by 2017, also provided an "escrow" service for transactions in crypto-currencies including Bitcoin, officials have said.

Medvedev was described as a co-administrator of the network, which was founded by Ukrainian hacker Svyatoslav Bondarenko, who remains at large.